MISSOURI DEPARTMENT OF MENTAL HEALTH

KEITH SCHAFER, DEPARTMENT DIRECTOR

DEPARTMENT OPERATING REGULATION NUMBER
DOR 8.390

CHAPTER	SUBCHAPTER	EFFECTIVE DATE	NUMBER OF PAGES	PAGE NUMBER
Regulatory Compliance	HIPAA Regulations	5-17-13	3	

SUBJECT	AUTHORITY	HISTORY
Risk Management	630.050 RSM0	See Below

PERSON RESPONSIBLE	SUNSET DATE
General Counsel	7-1-16

PURPOSE: The Department of Mental Health (DMH) recognizes the need to implement policies and procedures to prevent, detect, contain, and correct security violations to be in compliance with 45 CFR 164.308(a)(1)(i). DMH also is aware of the ongoing threat of data loss due to cyber crime and human error. The Risk Management program is designed to continually assess risk and adjust procedures accordingly by adding and/or changing data protections, keeping DMH staff trained and aware of their responsibilities regarding data protection, and reviewing policy and procedure.

APPLICATION: Applies to DMH, its facilities and workforce.

(1) Definitions:

(A) Breach: The unauthorized acquisition, access, use or disclosure of protected health information that compromises the security or privacy of such information, except where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information. HITECH Act Sec. 134000(1).

(B) Chief Security Officer (CSO): Individual designated to oversee all activities related to the development, implementation, maintenance of, and adherence to department and facility policies and procedures covering the electronic and physical security of, and access to, protected health information and other DMH data in compliance with federal and state laws and regulations.

(C) DMH Privacy Officer: The person officially designated to oversee all ongoing activities related to the development, implementation, maintenance of, and adherence to the Department of Mental Health Operating Regulations pertaining to the privacy of, and access to, protected consumer health information in compliance with federal and state laws and the Department of Mental Health's Notice of Privacy Practices.

(D) Health Insurance Portability and Accountability Act (HIPAA): Public Law 104-191 was enacted on August 21,1996 to establish standards for the privacy and security of protected health information. The rules that were promulgated to implement HIPAA can be found at 45 CFR Parts 160 and 164.

(E) Information Security Management Office (ISMO): The unit at the State of Missouri's Office of Administration responsible for monitoring the State of Missouri Computer network and notifying agencies of the State of Missouri's threat level.

(F) Local Security Officer (LSO): Individual designated to oversee facility information and physical security practice and policy compliance, and to coordinate those activities with the Chief Security Officer.

(G) Protected Health Information (PHI**)**: Individually identifiable health Information that is transmitted or maintained in any form or medium, by a covered entity, health plan or clearinghouse as defined under the Health Insurance Portability and Accountability Act (HIPAA), 45 CFR Part 160 and 164.

(2) Risk Management Program – DMH shall implement a risk management program to protect the confidentiality, integrity and availability of PHI.

(A) DMH shall assign a CSO to oversee data security and regulatory compliance;

(B) The protection procedures outlined in the DMH Security Maintenance Department Operating Regulation (DOR) 8.370 shall be followed by DMH employees and other state employees providing services to DMH;

(C) Risk assessments will be performed as described:

i. HIPAA security compliance will be performed by the DMH CSO annually.

ii. HIPAA privacy compliance will be performed by the DMH Privacy Officer annually.

iii. Existing information systems assessments will be performed when:

1. A change is proposed to the system's security components;
2. A major functionality update is performed;
3. New rules and/or regulations are introduced by state or federal government;
4. New technology is introduced;
5. New code sets are introduced into the system; or
6. Every three (3) years, whichever comes first.

iv. New information systems will be assessed for risk during the initiation stage of project.

(D) A training program shall be maintained as defined in DOR 8.090;

(E) DORs will be reviewed at least every three (3) years;

(F) Periodic site visits shall be completed by the CSO and/or DMH Privacy Officer at DMH facilities to review compliance;

(G) Bi-annual vulnerability assessments shall be performed on the computing infrastructure and hardware that host DMH systems performed by ISMO;

(H) Policy and procedure reviews shall be performed following any security incident that results in a breach of PHI;

(I) A current business continuity plan shall be prepared, approved and maintained by DMH;

(J) A disaster recovery plan for the computing infrastructure and hardware hosting DMH information systems shall be prepared and kept up to date by the provider of IT services and approved by DMH;

(K) Policies and procedures shall be in place to protect the physical security of staff and PHI;

(L) An annual inventory of computing equipment shall be performed;

(M) DMH employee Active Directory userIDs shall be audited quarterly as described in the DMH Employee userID Review Procedure attached;

(N) Mainframe userIDs will be audited quarterly. Mainframe userIDs not used in twenty-four (24) months will be deleted.
(O) DMH contract providers will be audited six (6) times annually. UserIDs associated with providers no longer under contract will be disabled.
(P) A provider audit shall be performed at least three (3) times annually as described in the Provider Account Audit procedure attached;
(Q) Access reports from CIMOR will be reviewed quarterly as described in the System Activity Review procedure attached; and
(R) Active Directory UserIDs will be deleted sixty (60) days after they are disabled.

(3) LOCAL POLICIES: There shall be no facility policies pertaining to this topic. The DMH DOR shall control.

(4) REVIEW PROCESS: The CSO shall collect information from the facility LSOs during the month of April each year to monitor compliance with this DOR.

(5) SANCTIONS: Failure of staff to comply or assure compliance with the DOR may result in disciplinary action, up to and including dismissal.

History: Original DOR effective May 17, 2013.

PROVIDER ACCOUNT AUDIT PROCEDURE – (2) (P)

Active Directory accounts shall be audited every four (4) months for inactivity on the provider domain for Providers accessing CIMOR. The ITSD Account Management Group will enforce that the Provider Local Security Officer (LSO) either submit paperwork for terminated employees or all Active Directory accounts that have been inactive for more than one hundred eighty (180) days will be disabled.

This procedure shall apply to all providers that have an Active Directory account on the provider domain to access CIMOR with one exception. Provider accounts with access to the Mortality Review application will not have their accounts disabled unless notification is received of their employment termination.

DEFINITIONS

Authorization Request Application (ARA): Automated security access request application for the CIMOR system.

PROCEDURE

1. In February, June and October, the ITSD Account Management Group will conduct an audit on all active DMH Provider Active Directory accounts to determine if each account has been used in the past one hundred eighty (180) days.

2. The ITSD Account Management Group will notify each provider LSO if that agency has any employees that have not logged on in the past one hundred eighty (180) days.

3. The Provider LSO is required to submit a DMH Contract Provider Access Request Form (http://dmh.mo.gov/itsd/cimor/index.htm) marked “REVOKED” for any terminated employees upon termination. If any terminated employees are on the audit list, a revoked form should be submitted immediately by fax to 573-526-6033.

4. If the employee is still employed with the Provider and the account has not been accessed in the past one hundred eighty (180) days, the ITSD Account Management Group will disable the account and note that the account has been disabled due to inactivity. The Provider LSO will be notified by email if any accounts for that agency have been disabled due to inactivity. As noted above, an exception will be made for Provider user accounts with access to the Mortality Review application. These accounts will not be disabled due to inactivity.

5. All CIMOR roles will also be removed if the account is inactive for more than one hundred eighty (180) days.

6. The Provider LSO will need to submit a new DMH Contract Provider Access Request Form to enable the Active Directory account for the employee to access CIMOR again.

7. An ARA request will need to be submitted to request CIMOR roles again.

SYSTEM ACTIVITY REVIEW PROCEDURE (2) (Q)

A system access review shall be performed on Department of Mental Health systems in accordance with HIPAA regulations.

DEFINITIONS

Audit Log: A permanent record that is written for every occurrence of a database record being accessed, updated, changed or deleted.
Access Report: Report generated out of an audit log for purposes of review.

PROCEDURE

1. Access reports from CIMOR will be reviewed quarterly. A random sampling of five (5) userIDs will be pulled from an access report to be examined. The five (5) will be chosen from a generated list of numbered CIMOR users. A randomizing program will provide the list number of the users to review.

2. The review will be performed by the CSO. The chosen userIDs will be verified against the CIMOR security database.

3. The audit log showing the last thirty (30) days of activity will be reviewed to ensure that the accesses made by the user are consistent with the user's security level and assigned job duties.

4. The user's roles will be compared to ensure that no incompatible functions are allowed for any user(s). This will be done from the security roles list.

5. The user's supervisor will be contacted to verify the type of security granted is in fact needed.

6. Any discrepancies found during this review will result in the appropriate change to the user's access. The corresponding security access request form will be submitted. The user's supervisor will be notified of any changes.

7. Discrepancies in access will be reviewed to identify patterns and to determine if changes to procedures are needed.

8. A report of each quarterly review will be maintained by the CSO.

9. Documentation will be located at: \\mzfileshare-v\hipaaproject\LB - Risk Management.

DMH EMPLOYEE USERID REVIEW PROCEDURE (2)(M)

A system access review shall be performed by the CSO on DMH employee userIDs quarterly. This shall include user access to Active Directory as well as other agency systems including, but not limited to, SAM II systems.

DEFINITIONS

Active Directory: The statewide network authentication system serving Missouri state agencies.

SAM II: The financial and human resources computer systems used by Missouri state agencies.

PROCEDURE

1. A list of DMH employee userIDs not used for sixty (60) days, yet still enabled in Active Directory, will be generated annually.

2. The list will be sorted by facility and sent to each facility's Human Resources contact for verification.

3. UserIDs for terminated DMH employees shall be immediately disabled in Active Directory by submitting a Help ticket to the ITSD Account Management Group.

4. System access requests marked "revoke" will be sent to the appropriate agency for any terminated DMH employee userIDs.

5. If agency systems, such as SAM II, provide a list of current users, the list will be verified against Active Directory to ensure all system users are still employed.

6. Sixty (60) days after userIDs are disabled they will be deleted from Active Directory.

7. A report of each review will be maintained by the CSO.

PROVIDER REVIEW & REPORT TO SSA

The Missouri Department of Mental Health (DMH) receives social security number information from the Social Security Administration (SSA) as part of a defined verification process. The contract in place that allows this exchange of data requires DMH to periodically notify SSA of all persons with access to the data SSA provides.

This document provides the procedures to accomplish that requirement.

PROCEDURE

1. DMH ITSD has written a computer program that triggers bi-monthly on:

January 15
March 15
May 15
July 15
September 15
November 15

The report is a snapshot of the providers on the report run date taken from the CIMOR database. The report is emailed to the CSO, ITSD Account Management, and report programmers.

2. ITSD Account Management Group checks the spreadsheet for the current reporting period.

A. If there is no contract end date, this is a current provider.
B. If there is a contract end date noted, all user accounts for that provider must be disabled.
C. A report of all changes is emailed to the CSO.

3. After reviewing and changing the latest report, the CSO will send it to SSA along with the *Contract_Provider_SSA_Service_Category_Definitions_2009[1]* document located at My Documents/SSA folder. These should be sent to Michelle Palmer (Michelle.Palmer@ssa.gov).

4. The CSO will forward the sent email to Cathy Welch and request she email the letter on behalf of the director to the SSA, and copy the Regional Commissioner for the SSA, Ken Powell. Email the letter to ||KC ORC (KC.ORC@ssa.gov) with a copy to ||KC CPS (KC.CPS@ssa.gov).